Retaliatory Strikes as a Reaction to Cyber-Attacks?

The recent Israeli Airstrike against HamasCyberHQ from an IHL perspective

---

Völkerrechtsblog 2019-05-22T11:07:38

Between Friday (3 May 2019) and Sunday (5 May 2019) violence erupted again between Israel and the Palestinians led by governing Hamas in the Gaza Strip. In the course of a severe exchange of violence between the two conflict parties, the Israel Defense Forces (IDF) conducted a physical attack countering an offensive cyber operation by Hamas. According to IDF, the air strike was conducted against the Hamas Cyber Headquarter and a reaction to a cyber operation. Some accounts took this information up and claimed a precedent, arguing that it was the first time a nation reacted to an ongoing cyber operation with a physical strike. In the following I will discuss some of the relevant questions of the law of armed conflict (LOAC) and show that the airstrike does not constitute a legally relevant precedent.

Applicability of Law of Armed Conflict

International humanitarian law and/or LOAC is applicable in international and/or non-international armed conflicts (common Art. 2 GC I-IV, Art. 1 (3), (4) AP I– int. armed conflict; and Art. 3 GC I-IV, Art. 1 AP II– non-int. armed conflict). Both legal frameworks have nearly identical basic sets of rules, which are accepted as customary international law. At least the cardinal principles of humanitarian law – the principle of distinction and the prohibition to cause unnecessary suffering – are in common.

Without prejudice about the legal status of the Gaza Strip the applicability of the LOAC requires an armed conflict. According to the definition of an armed conflict by the ICTY the exchange of rockets, artillery fire and the air strikes between the conflict parties constitute protracted armed violence between governmental authorities of Israel and the Hamas as organized armed group – OAG. Besides the highly controversial topic of 'Palestine' as a State, the Gaza Strip and the governing Hamas predominantly are not considered as a State on their own. Thus, the conflict most likely is non-international. In any case the conflict amounted to the necessary level for the applicability of LOAC and the cardinal principles.

Applicable Rules to Airstrikes

Besides the rules of the weapons law, meaning the rules that prohibit certain types of weapons and their effects, compare Art. 35 (2) AP I, Art. 51 (4) lit. b and c AP I and Art. 35 (3) AP I the legality of airstrikes is governed by the so called '*targeting law*'. The term refers to the set of rules which regulate attacks directed at a certain target.

Art. 57 AP I contains a paradigmatic targeting process in accordance with LOAC. *Inter alia* the following rules have to be respected concerning airstrikes.

Attacks on targets in an area where civilians live, in particular, have to respect the principle of distinction. The principle obliges to differentiate between civilians and combatants, civilian objects and military objectives, thus, between unlawful and lawful targets (Art. 48, 51 and 52 AP I).

According to Art. 51 (3) AP I civilians shall be protected and attacks may not be directed at them, unless and for such time as they directly take part in hostilities (the Direct Participation in Hostilities Rule or '*DPH-Rule*'). Civilians which directly participate in hostilities become a lawful target for the duration of their participation. When they fulfill a continuous combat function this loss is retained. Members of OAGs generally are assumed to have a continuous combat function and may be attacked at all times just the same as regular combatants (compare the ICRCs DPH study).

Likewise, originally civilian objects that are used for military purposes can be attacked. On the other side it is prohibited to hide military targets between civilians, in civilian objects (Art. 58 AP I) and to use civilians as protective shields against attacks (Art. 51 (7)AP I). It constitutes a violation of LOAC if protected areas or objects like hospitals, mosques, schools (…) are abused for military gains as in Art. 51 (7), 54 (3), 58 AP I.

Before and during the attack certain precautions have to be taken. Especially in inhabited areas warnings should be issued before an attack, see Art. 57 AP I.

Finally attacks are prohibited if they may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects (…), which would be excessive in relation to the concrete and direct military advantage anticipated, see Art. 57 (2) (a) (iii) AP I. Therefore, parties of a conflict are obliged to use a minimum of force in civilian surroundings.

The Airstrike against HamasCyberHQ

Concerning the airstrikes from the 5th of May there is no information about the weapons used by the IDF, neither are there confirmed information about the specific content, course and effects of the Hamas cyber operations. Thus, solely targeting law can be evaluated here.

The airstrikes have been conducted against a building in the Gaza Strip, which is a densely populated area. Hence, LOAC obliges to use special care and a minimum of force if attacks are conducted in such civilian surroundings. The IDF air force claims to use smart bombs and precision-guided munition (PGM) in airstrikes.

Hamas and its Members under LOAC

If Hamas is seen as government of a State, the members of their armed groups are considered as combatants. An attack on them would be lawful, provided the

aforementioned other rules are complied with. If they are seen as an OAG, their armed members become lawful targets due to their continuous combat function, see Art. 51 (3) AP I.

Other Hamas members who do not carry out a combat function – as the organization has political components, too – possibly may be classified as civilians. However, the organization has a military or paramilitary background. It is therefore hard to distinguish political members from the ones who are part of the armed groups. When a person originally classified as civilian takes up a weapon and gets involved in the fighting, it becomes a lawful target due to Art. 51 (3) AP I. *De minimis* members with military or semi-military function are seen as lawful targets either due to Art. 43 (2), 48 AP I or due to Art. 51 (3) AP I.

The known problems and discussions concerning the criteria and thresholds of the DPH rule are raised by the status of Hamas members. What about persons who fulfill supply, governance or executive functions? The fine line between lawful targets and protected civilians is blurred on various occasions.

The Case of the HamasCyberHQ

To the extent known, the building which was the object of the airstrike was located in a civilian area. If the nature or purpose of the object does not make an effective contribution to military action, it shall be presumed to be used for civilian purposes as a rule of doubt (Art.52 (2), (3) AP I). Therefore, the nature and purpose of the HamasCyberHQ is decisive for the lawfulness of the strike. This depends on the actual contribution to military action and, thus, on the purpose and function by the personal residing there. In addition, the functions and activities of the personal determine their legal status. If they have to be qualified as protected persons, this might constitute a reason for the unlawfulness of the strike in connection with the proportionality rule.

Provided the building was a base for the intelligence branch and the HamasCyberHQ, their functions must have contributed to the military activities. The intelligence branch regularly serves not only internal purposes but external, cross-border purposes. With a view to the continuously ongoing conflict with regular armed clashes with Israel, it is highly likely that it includes a military component. The military intelligence branch gains military advantage for Hamas when military intelligence is gathered about Israel. Due to this function it becomes a military object. Therefore, an attack against the intelligence service offers a military advantage and is lawful, see Art. 51, 52 AP I.

Cyber Operatives

Concerning cyber operations, the capability and functions of the cyber operatives have to be analyzed. If they conduct harmful cyber operations which can cause physical effects and destruction, especially if they can affect Israeli military operations, the cyber operatives do not have to be treated different than regular participants in armed operations. An example might be a cyber operation that interferes with military communication of the opponent.

Persons linked to an OAG, who are able to affect military operations of another conflict party, execute military functions. Cyber operatives tasked accordingly, have to be classified likewise. If they are affiliated with an OAG, they clearly have a continuous combat function. If they are not a member or part of an OAG and they perform their operations as civilians, they nevertheless directly participate in hostilities. It does not matter whether the personal in question solely works on a computer in distance to the '*real*' fighting, as long as they contribute to the military efforts of a party to the conflict. Hereto the type, the function and the (intended or possible) effects of the cyber operation become decisive for the legal status.

Cyber Operations

As cyber operations can have various functions and often are 'dual-use' the distinction becomes more problematic. Many grey zones or at least close single cases arise as a 'civilian' DDOS attack (= Distributed Denial of Service Attack) can have an effect on a military operation. Thus, the lowest threshold with view to LOAC and in connection to the ongoing armed conflict has to be identified: This is any cyber operation that fosters the military operation, helps it to be more effective and consequently provides a military advantage. The cyber operation always has to be compared to conventional operations and non-sufficient support operations.

Inter alia DDOS attacks, the infiltration of military or governmental networks and computers with military (guidance) connection, the change of military or governmental data and the interference with signals can be qualified as a military advantage towards the other party. Besides information operations like publishing or otherwise spreading misleading information for enemy forces create military gain. Also a misinformation about the military status of a civilian object, which additionally leads to an abuse of the civilian protection status, constitutes another violation of Art. 51 AP I.

In conclusion, the lawfulness of the attack on the HamasCyberHQ depends on the single facts of the case and thereby on the type of the conducted cyber operation(s). In case the cyber operatives have or had conducted a cyber operation against Israel as claimed by the IDF, it is not farfetched that the operation was intended to create relevant military gain for Hamas. An attack against the cyber operatives therefore would have been lawful with view to the status of the HamasCyberHQ. Nevertheless, this can only be determined in the end if some 'hard' facts of the defended cyber operation are published. The same is true for other legal requirements of the airstrike like the proportionality rule and the duty to precautions. These cannot be assessed without further information.

Prospects of Cyber Operations under LOAC

The incidents of the first weekend of May 2019 again demonstrate how fast the conflict between Israel and Hamas can escalate. It also shows that both parties are ready and willing to use all available tools to defeat the other party. The open statement on a cyber operation against Israel, its defense by the IDF and the thereby justified conventional airstrike on the HamasCyberHQ present a variety of legal issues from LOAC perspective. Most of these questions derive from already existing

legal discussions about the content and interpretation of LOAC. Nonetheless, the peculiarities of the conduct of cyber operations, their functions and their effects lead to new grey zones. There is an urgent need for further clarification by States on their interpretation and categorization of cyber operations to prevent an escalation of violence in reaction to cyber operations. In the present case on the basis of the available information a violation of LOAC has probably not taken place. However, if not in this case – the next airstrike against cyber operatives in a populated area can cause civilian victims and violate LOAC.

Dr. iur. Tassilo Singer is a Trainee Lawyer at the District Court of Traunstein, Germany and a former research associate at the European University Viadrina (Prof. Heintschel von Heinegg) and University of Passau (Prof. Dederer). He is furthermore guest lecturer at the Masaryk University Brno (ELSA Summer School on IT Law).

Cite as: Tassilo Singer, “Retaliatory Strikes as a Reaction to Cyber-Attacks? The recent Israeli Airstrike against HamasCyberHQ from an IHL perspective”, *Völkerrechtsblog*, 22 May 2019.
